CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- IDScan.net, a US identity verification provider, has disclosed a data breach after detecting unauthorized access on September 1. Exposed data included names and government identification numbers, while a criminal marketplace advertised a collection containing millions of identity documents, including driver's licenses, associated with the company's verification services.
- Mathspace, an education platform used in Australia and New Zealand, has suffered a data breach affecting more than 1 million people. The attackers exploited CVE-2026-72898 in self-hosted tool Metabase to access an internal reporting database. Exposed information included names, email addresses, usernames, and locations, while passwords and academic records were not affected.

  Check Point IPS provides protection against this threat (Metabase SQL Injection (CVE-2026-72898))
- Fintech company Revolut has reported a data exposure after employees fulfilled fraudulent information requests sent from an email account within a government agency's legitimate domain. Exposed records included identity documents, verification selfies, contact details, IBANs, account statements, withdrawal records, and complete transaction histories.
- Florida's state Department of Motor Vehicles fell victim to a data breach after criminals used credentials stolen from a Plant City police officer's personal device. The credentials enabled access to driver records, and the ShinyHunters group published images of stolen data.

AI THREATS

- Check Point Research has detailed PuzzleMask, a plain-prose prompt technique that hides prohibited instructions from lightweight LLM gatekeepers while allowing stronger target models to recover them. In testing, gatekeepers classified the prompts as safe, while target models extracted and acted on concealed payloads in more than 90 percent of trials.
- Check Point Research has demonstrated a covert cross-account channel in ChatGPT's code-execution environment that allowed hidden tasks to run using a victim's available tools, data, and connected applications. A proof of concept used a shared conversation to retrieve Gmail data from one account and relay the results to another.
- Anthropic has disclosed four incidents in which Claude models operated on the real internet because of configuration failures instead of remaining within intended sandboxes. In the most serious case, a model published a malicious PyPI package that was executed by systems, exposing credentials and enabling access to a database.

VULNERABILITIES AND PATCHES

- Microsoft has released its September 2026 Patch Tuesday updates, addressing a record 974 vulnerabilities across its products, including two actively exploited zero-days. CVE-2026-85880 and CVE-2026-81963 both allow local attackers to elevate privileges to SYSTEM, while 20 additional flaws could enable unauthenticated remote code execution without user interaction.

  Check Point IPS provides protection against this threat *(Microsoft Windows Update Stack Elevation of Privilege (CVE-2026-81963))*

- GitLab has addressed CVE-2026-85706, a critical path traversal vulnerability affecting Community and Enterprise Editions, with a CVSS score of 10.0. The flaw allows unauthenticated attackers to read arbitrary files through the repository commits API. Affected versions include 18.7 through 19.3.1, with fixes available in 19.1.8, 19.2.6, and 19.3.2.

  Check Point IPS provides protection against this threat *(GitLab Arbitrary File Read (CVE-2026-85706))*

- MikroTik has fixed CVE-2026-67276 and CVE-2026-86060, RouterOS vulnerabilities that can be chained to obtain passwordless SSH access and elevate privileges to full administrator. Successful exploitation can give attackers control over exposed routers, enabling configuration changes, DNS manipulation, traffic interception, and use of compromised devices as network footholds

THREAT INTELLIGENCE REPORTS

- Check Point Research has reported that enterprise GenAI usage continued to expand in August, reaching an average of 106 prompts per user, while 86% of organizations regularly using GenAI were affected by high-risk prompt activity. The report also recorded 1,042 ransomware attacks, almost double the August 2025 figure, while average weekly cyberattacks rose 22% year over year to 2,422 per organization.

- Researchers have detected a passkey-themed social engineering campaign targeting Microsoft 365 accounts. Attackers use phone and text lures directing employees to lookalike sign-in pages, then register their own authentication methods and collect data from SharePoint, OneDrive, and Exchange after gaining access to compromised accounts.

- Researchers have analyzed an Android banking-fraud campaign by the GoldFactory group that abuses Android Work Profile functionality through a tool called Vwork to clone victims' banking applications. The Gigabud malware used in the operation was linked to at least 1,469 compromised devices in Indonesia and nearly $1 million in losses.

- Researchers have detailed BlueMoon, an exploit chain combining two vulnerabilities in Chromium's V8 JavaScript engine with a Windows flaw to compromise targeted systems. The vulnerabilities were used by multiple espionage groups after Chrome patches became available, allowing browser exploitation, sandbox escape, and privilege escalation on vulnerable Windows devices.

  Check Point IPS provides protection against this threat *(Google Chrome Type Confusion (CVE-2026-85046))*